
# Command, Control, Communication, Computers and Information Technology (C4&IT)

## Strategic Plan

FY 2008 - 2012

# Report Documentation Page

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE | 2. REPORT TYPE | 3. DATES COVERED |
|---|---|---|
| **2008** | | **00-00-2008 to 00-00-2008** |

| 4. TITLE AND SUBTITLE | 5a. CONTRACT NUMBER |
|---|---|
| **Command, Control, Communication, Computers and Information Technology (C4&IT)** | 5b. GRANT NUMBER |
| | 5c. PROGRAM ELEMENT NUMBER |
| 6. AUTHOR(S) | 5d. PROJECT NUMBER |
| | 5e. TASK NUMBER |
| | 5f. WORK UNIT NUMBER |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Coast Guard,Washington,DC** | 8. PERFORMING ORGANIZATION REPORT NUMBER |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSOR/MONITOR'S ACRONYM(S) |
| | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) |

12. DISTRIBUTION/AVAILABILITY STATEMENT
**Approved for public release; distribution unlimited**

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT **unclassified** | b. ABSTRACT **unclassified** | c. THIS PAGE **unclassified** | **Same as Report (SAR)** | **60** | |

To the Men and Women of the Coast Guard:

I am pleased to present the U.S. Coast Guard's *Command, Control, Communication, Computers, and Information Technology (C4&IT) Strategic Plan for Fiscal Years 2008-2012*. Driven by the overarching goals of the Department of Homeland Security (DHS) and the Coast Guard, this plan charts an ambitious course for our C4&IT capabilities over the next five years.

Information is a key enabler for Coast Guard mission success. To save lives, safeguard our maritime borders, respond to natural and man-made disasters, interdict illegal drugs, and move commerce across the high seas, we need C4&IT to seamlessly communicate and share information.

To meet these mission demands, this plan charts the way ahead by identifying goals, objectives, and initiatives in the core areas listed below. By targeting our C4&IT efforts in each of these areas, we can focus on immediately improving mission support while creating a foundation for future enhancements.

| | |
|---|---|
| Information: | Improve and encourage information sharing, quality, efficiency, and compliance throughout the Coast Guard. |
| Technology: | Deliver mission-focused, interoperable, innovative, and net-centric C4&IT using enterprise-wide solutions, an optimized infrastructure, and electromagnetic spectrum efficiency. |
| Security: | Prevent C4&IT security issues, such as cyber attacks and intrusions, and enhance C4&IT security mitigation, recovery, awareness, and compliance. |
| Governance: | Enhance C4&IT governance to meet requirements and encourage effective enterprise architecture, capital planning and investment control, systems development life cycle, project management, and performance measurement processes. |
| Organizational Excellence: | Achieve organizational excellence and provide superior customer service by continually developing our workforce, reaching out to internal and external stakeholders, and improving business processes. |

This plan serves the Coast Guard on several levels. For Coast Guard men and women deployed throughout the world, this strategy lays the foundation for C4&IT capabilities that will help them meet new challenges. For Coast Guard leaders, it signals our ongoing commitment to formulating an actionable and measurable C4&IT strategy that aligns with mission execution. For our C4&IT employees, it shows how their contributions support the broader vision for Coast Guard C4&IT.

The success of this C4&IT strategy depends on the talents, commitment, and proactive involvement of the entire Coast Guard community. We look forward to continuing to work with all of our stakeholders to achieve our mutual goals of maritime safety, security, and stewardship.

Rear Admiral David T. Glenn
*Assistant Commandant for C4 & Information Technology,*
*Chief Information Officer*
United States Coast Guard

Intentionally Blank

## Table of Contents

# INTRODUCTION

## PURPOSE

The Assistant Commandant for Command, Control, Communications, Computers, and Information Technology (C4&IT)/CG-6, Chief Information Officer (CIO), for the Coast Guard publishes this C4&IT Strategic Plan. The purpose of this plan is to provide a unifying strategy to better integrate and synchronize Coast Guard C4&IT and maximize operational capabilities.

## SCOPE

This plan is intended to be used cooperatively by members of the C4&IT community to establish and prioritize recommendations for implementing improvements to the Coast Guard's C4&IT infrastructure and enterprise applications, and processes for information assurance, enterprise architecture, data privacy, and resource management. The focus of this document is on activities that must occur in the next five years to progress toward achieving the long term goals of the Coast Guard and the Department of Homeland Security (DHS). While the end-state goals in this plan may not be fully realized in the next 5 years, it is clear that coordinated activity must occur now to improve the Coast Guard's operational capabilities.

## AUTHORITY

The C4&IT Strategic Plan has been developed under the authority of the Assistant Commandant for C4&IT, CIO, for the Coast Guard. CG-6 derives its authority for C4&IT from COMDINST 5401.5, Establishment of the CG-6 Directorate and Associated Duties, which made CG-6 the office responsible for all Coast Guard operational, business, and infrastructure C4&IT assets.

At a departmental level, DHS Management Directive (MD) 0007.1, Information Technology Integration and Management, establishes the component CIO as the authority responsible for the timely delivery of Information Technology (IT) mission services and effective management and administration of all component IT resources. In addition, DHS MD 0007.1 states that the component CIO is responsible for effective management and administration of all component IT resources and assets to meet mission, departmental, and enterprise program goals.

At a Federal level, U.S. Code Title 44, Public Printing and Documents, Federal Information Policy mandates that the CIO develop and maintain a strategic information resources management plan; establish goals for improving the contribution of information resources to program productivity, efficiency, and effectiveness; and identify methods for measuring progress towards reaching those goals. This plan addresses each of these federally mandated responsibilities.

# BACKGROUND

## CURRENT ENVIRONMENT

The U.S. Coast Guard, one of the nation's five armed services, is the principal Federal agency responsible for maritime safety, security, and stewardship. As such, we protect the vital economic, environmental, and security interests of the United States. This includes the personal safety and security of the maritime public, our natural and economic resources, the global commerce infrastructure, and the integrity of our maritime borders. We are committed to addressing all threats and hazards in a manner consistent with the law and in alignment with the goals and objectives of DHS. We do this throughout the maritime domain including in U.S. ports and inland waterways, along the coasts, on the high seas, and in other regions where our maritime equities are at stake.

> "OUR FUTURE LIES IN A FLEXIBLE, AGILE AND MODERN FORCE."
>
> - ADM Allen,
> Commandant,
> U.S. Coast Guard

As a military, multi-mission, and maritime service, we have three fundamental roles: maritime safety, security, and stewardship. In each of these roles, the Coast Guard depends on C4&IT to achieve its missions.

From Miami to Juneau, in Coast Guard command centers across the United States, we use C4&IT systems to capture information about suspicious activities and possible threats. On our 200 ships, 250 aircraft, and 1,700 boats, we deploy C4&IT assets, such as radios and sensors, to keep our forces connected with internal and external partners on shore, along the coasts, and on the high seas. Supporting the missions of the Coast Guard, our 89,000 military, civilian, and auxiliary employees use over 42,000 computers, 350 applications, and 780 C4&IT products to perform their work each day.

## CHALLENGES

We operate in a continually changing and complex mission environment. As such, the way ahead poses many challenges for the Coast Guard. This is especially true in the area of C4&IT as the Coast Guard becomes more dependent on technology for mission execution. As the Directorate for C4&IT (CG-6), we must adapt our goals, objectives, and initiatives to fulfill the Coast Guard's complex and continually changing mission and business needs.

The following sections outline some of the challenges that we currently face as the Coast Guard's Directorate for C4&IT.

- Balance Between Missions: After September 11, 2001, the Coast Guard's priorities and focus shifted suddenly and dramatically. Today and into the future, as a component of DHS, the Coast Guard must dedicate more resources to homeland security missions. In addition, any unexpected event, from a man-made disaster (such as a terrorist attack) to a natural disaster (such as a hurricane), may result in a shift in resources. Further complicating this balance between missions is the understanding that the Coast Guard, as a military service, must remain

ready and prepared to respond to the needs of the Department of Defense (DoD). To fulfill these varied roles, we must ensure that our technology is agile and mission-focused.

- Interoperability with Partners: The Coast Guard must be able to effectively interoperate and share information across a wide range of inter- and intra-agency partners to support disaster relief, law enforcement, defense, and other mission-related areas. This demand for information sharing and interoperability is not a new issue. Previous events, such as Hurricane Katrina, prove that information sharing and interoperability can lead to mission success. Consequently, we must implement compatible equipment and standards, and define procedures and practices for information sharing to ensure seamless communication with our partners.

- Increasing Demands Against a Relatively Constant Budget: User expectations and requirements continually increase as technology advances. At the same time, the overall funding available for C4&IT investment remains relatively constant. As demands increase, we must improve our ability to prioritize investments to achieve maximum results with our scarce resources.

- Increasing Threats to Network and Information: From capturing intelligence about a possible threat to transmitting employee information, we rely on our network to exchange, process, and store information 24 hours a day, seven days a week. At the same time, the gap between identifying a network vulnerability to the time of adversary exploitation has narrowed. As a result, we must protect and defend this vital resource to assure network and information confidentiality, integrity, availability, and privacy at all times.

- Rapid Pace of Technology Advancement: Technology is progressing at an ever increasing pace. This represents a significant challenge and opportunity for the Coast Guard. As we advance, we must balance the incorporation of new technologies that improve our operational capabilities with our limited resources and funding. We must be prepared to provide innovative services to our customers by re-thinking our current C4&IT approaches in light of technology advancements.

- Rising Customer Expectations: As new technology becomes available and commonplace in the market, Coast Guard personnel continue to find new ways leverage C4&IT to perform their jobs more effectively. In addition, interacting with agencies that have newly fielded capabilities can often intensify our employees' interest in new technologies. As technologies advance, we must make informed decisions about how to deploy new capabilities to maximize Coast Guard effectiveness and fulfill customer expectations.

These are but a few of the challenges that the Coast Guard must address. Our ability to select the appropriate strategies to meet these challenges will help to enable Coast Guard success in the future. Implementing this C4&IT Strategic Plan, and the related CG-6 Performance Plan (Appendix A), will enable systematic and comprehensive resolution of these challenges.

## STRATEGIC GUIDANCE

By understanding and aligning our goals to Federal, DHS, and Coast Guard strategic guidance, we can enhance Coast Guard mission execution. Figure 1 shows how Federal, DHS, and Coast Guard guidance shaped the goals, objectives, and initiatives identified later this plan. Highlighted at the top of each box in Figure 1 are the specific guidance documents that we discuss in more detail in the following sections.

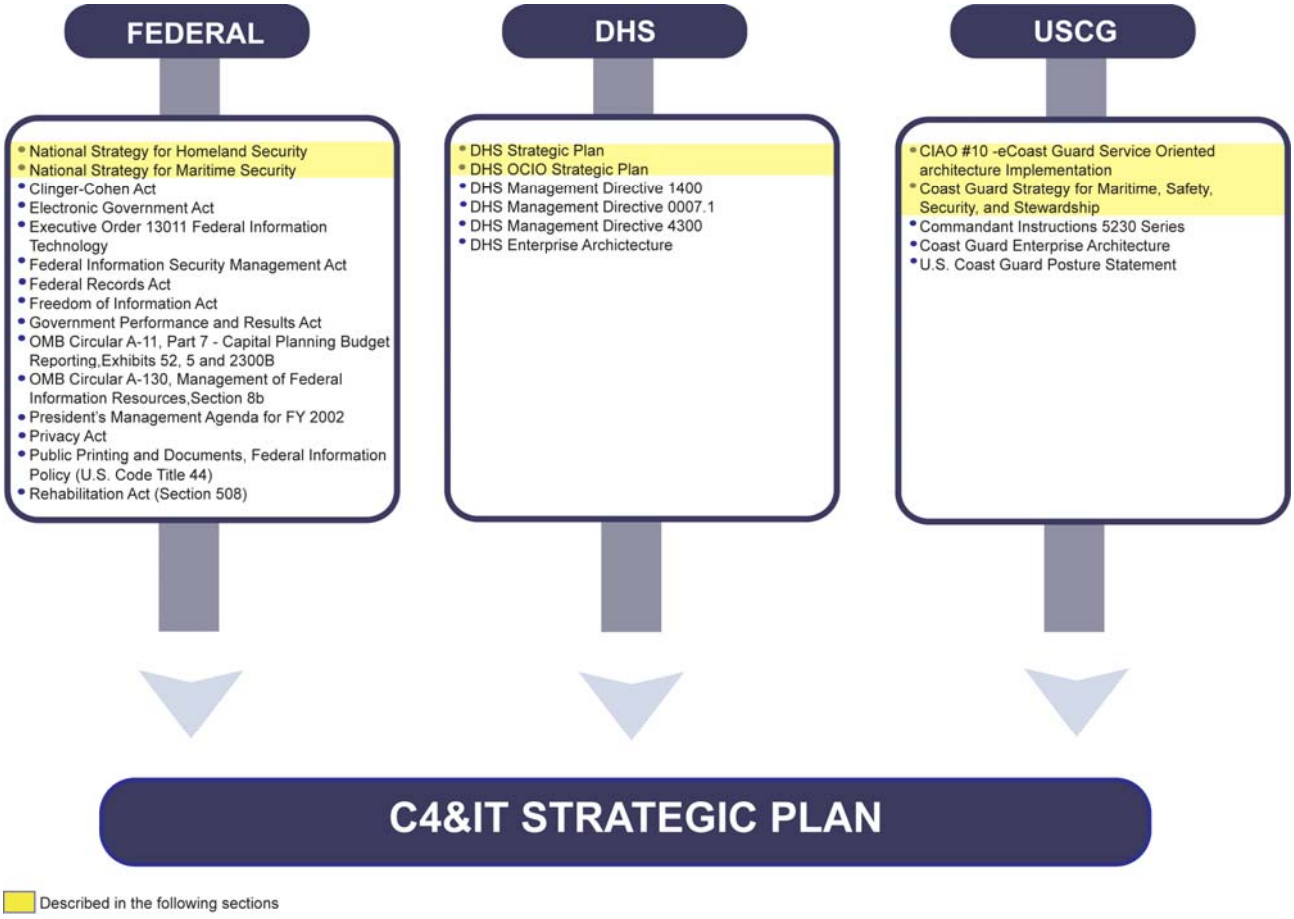


**Figure 1: C4&IT Strategic Plan Guidance**

### Federal Guidance

The *National Strategy for Homeland Security* serves to guide, organize, and unify our Nation's homeland security efforts. It recognizes that we must continue to focus on the persistent and evolving terrorist threat while addressing the full range of potential catastrophic events, including man-made and natural disasters, that impact homeland security.

The following goals from the *National Strategy for Homeland Security* guide the Nation's homeland security activities:

- Prevent and disrupt terrorist attacks;
- Protect the American people, our critical infrastructure, and key resources;
- Respond to and recover from incidents that do occur; and

- Continue to strengthen the foundation to ensure our long-term success.

In addition, the *National Strategy for Maritime Security* (NSMS) serves to integrate and synchronize the existing DHS strategies for maritime security and ensure their effective and efficient implementation. The following objectives from the NSMS guide the Nation's maritime security activities:

- Prevent Terrorist Attacks and Criminal or Hostile Acts: Detect, deter, interdict, and defeat terrorist attacks, criminal acts, or hostile acts in the maritime domain, and prevent its unlawful exploitation for those purposes.

- Protect Maritime-Related Population Centers and Critical Infrastructures: Protect maritime-related population centers, critical infrastructure, key resources, transportation systems, borders, harbors, ports, and coastal approaches in the maritime domain.

- Minimize Damage and Expedite Recovery: Minimize damage and expedite recovery from attacks within the maritime domain.

- Safeguard the Ocean and Its Resources: Safeguard the ocean and its resources from unlawful exploitation and intentional critical damage.

## Department of Homeland Security (DHS) Guidance

The United States Government established the Department of Homeland Security to secure the American homeland and protect the American people. The *DHS Strategic Plan* interprets the *National Strategy for Homeland Security* and prescribes the homeland security vision for the DHS workforce, DHS stakeholders, and the American people. The following goals from the *DHS Strategic Plan* guide the breadth of our activities at the Coast Guard.

- Awareness: Identify and understand threats, assess vulnerabilities, determine potential impacts, and disseminate timely information to our homeland security partners and the American public.

- Prevention: Detect, deter, and mitigate threats to our homeland.

- Protection: Safeguard our people and their freedoms, critical infrastructure, property, and the economy of our Nation from acts of terrorism, natural disasters, or other emergencies.

- Response: Lead, manage, and coordinate the national response to acts of terrorism, natural disasters, or other emergencies.

- Recovery: Lead national, state, local, and private sector efforts to restore services and rebuild communities after acts of terrorism, natural disasters, or other emergencies.

- Service: Serve the public effectively by facilitating lawful trade, travel, and immigration.

- Organizational Excellence: Value our most important resource, our people. Create a culture that promotes a common identity, innovation, mutual respect, accountability, and teamwork to achieve efficiencies, effectiveness, and operational synergies.

Specifically for IT, the DHS CIO established five strategic goals for enhancing the Department's IT capabilities in support of the mission objectives of DHS. These goals, as identified in the *DHS Office of the CIO (OCIO) Strategic Plan,* are:

- Goal 1: Continue cyber security improvements.
- Goal 2: Drive IT operational efficiencies, improvements, and resiliency.
- Goal 3: Align IT planning and budgeting with the procurement activities and the enterprise architecture.
- Goal 4: Establish a foundation for information sharing, data collection, and integration.
- Goal 5: Establish and govern a portfolio of cross-departmental IT capabilities to support DHS mission and management objectives.

The C4&IT Strategic Plan closely aligns with the DHS CIO's goals for the Department (see Appendix B for matrices). The alignment of these two sets of goals helps to ensure that the Coast Guard's C4&IT goals and objectives fully support the Department's goals. This alignment also provides opportunities to collaborate with the other components within DHS as they work to achieve the same goals.

## U.S. Coast Guard Guidance

In 2007, ADM Thad Allen published the *Coast Guard Strategy for Maritime, Safety, Security, and Stewardship*. This strategy is the framework and strategic intent that guides the Coast Guard's actions. More specifically, it identifies the following priorities for improving the Nation's preparedness and advancing U.S. maritime interests.

- Strengthening Regimes for the U.S. Maritime Domain: The Coast Guard will work with DHS, interagency partners, U.S. maritime stakeholders, and the international community to update and strengthen existing maritime regimes and put in place new regimes where needed to address emerging challenges and threats.
- Achieving Awareness in the Maritime Domain: The Coast Guard will work with the DoD, U.S. interagency partners, state and local governments, the private sector, and the international community to implement the *National Plan to Achieve Maritime Domain Awareness* as intended by the NSMS.
- Enhancing Unity of Effort in Maritime Planning and Operations: The Coast Guard will improve its integrated planning with all partners, its network of command and control centers, and its operational capabilities. In doing this, the Coast Guard will advance unity of command where possible, and unity of effort at all times. The Coast Guard will also align its operational structure around shore based, maritime patrol, and deployable specialized forces to better allow force packaging and scalable response to all threats and all hazards. This will support the NSMS and its *Maritime Operational Threat Response Plan* (MOTR), as well as the *National Response Plan*.

- Integrating Coast Guard Capabilities for National Defense: The Coast Guard will better integrate its capabilities with DoD and optimize its forces within a Navy/Coast Guard relationship. This will build upon the "National Fleet" model and support the *National Maritime Strategy* (NMS) as well as the NSMS and its subordinate plans.

- Developing a National Capacity for Maritime Transportation System Recovery: To support the NSMS and its *Maritime Infrastructure Recovery Plan* (MIRP), the Coast Guard will leverage its authorities, responsibilities, and capabilities to lead the national planning agenda for assuring the continuity of commerce and critical maritime activities.

- Focusing International Engagement on Maritime Governance: The Coast Guard will focus its international efforts to assist maritime organizations and partner nations in building the sustainable regimes, awareness, and operational capabilities necessary to improve the governance of the global maritime domain.

Additionally, as part of the Commandant's Intent Action Orders (CIAOs), the Commandant mandated the implementation of e-Coast Guard (eCG) and Service Oriented Architecture (SOA) (CIAO #10). The goal of this mandate is to enhance Coast Guard mission performance through optimal C4&IT investments and management. Many of the objectives and initiatives described in this plan focus on building the momentum needed to develop, deploy, support, and sustain SOA for our IT projects. This includes developing policies, practices, procedures, and tools to enforce and encourage information sharing, technology standards, and the development of loosely coupled, mission-focused systems.

# CG-6 MISSION & VISION

## MISSION

The Assistant Commandant for C4&IT/CG-6 designs, develops, deploys, and maintains C4&IT solutions for the entire Coast Guard to enable mission execution and achieve the Coast Guard's goals of maritime safety, security, and stewardship.

## VISION

A Coast Guard ready with the right information at the right time to safeguard the Nation's maritime domain.

## CORE VALUES AND CONCEPTS

Interrelated core values and concepts guide the way we, as CG-6, conduct business. These core values and concepts are summarized below:

- C4&IT Leadership: We believe that C4&IT leaders set clear technology direction, have high expectations for system delivery, create a customer-focused culture, and balance the needs of all stakeholders to ensure that we meet mission requirements. C4&IT leaders inspire their workforce and motivate them to grow professionally, contribute wholly, and be creative.

- Visibility and Transparency: We believe that all aspects of C4&IT management must be visible and transparent to CG-6 system managers, as well as stakeholders, at all times during system planning, development, and support. Visibility and transparency are particularly important to C4&IT spending and system performance. To this end, we support a collaborative investment management process that gives the entire organization access to C4&IT priority decisions.

- Guidance: We believe in establishing guidelines that ensure organizational agility and effective acquisition, application, and management of C4&IT systems through a policy and practices framework, and interactions with stakeholder organizations. Our guidelines provide an appropriate level of discipline and structure, and identify the necessary tools to deliver timely and reliable C4&IT systems in an unprecedented way.

- Optimizing Outcomes: We believe in leveraging C4&IT to accomplish the Coast Guard's missions and deliver superior results. We recognize the extraordinary value of innovation when employees apply an entrepreneurial spirit by using technology as a performance enabler. With this in mind, we established the Enterprise Architecture (EA), Systems Development Life Cycle (SDLC), and investment management processes with maximum flexibility to ensure that technology ultimately improves Coast Guard mission and program performance.

- Partnering to Accomplish the Coast Guard Missions: We believe that no CG-6 activity can operate in isolation of Coast Guard operational missions and programs. Our success and ability to add value depends upon the ability of CG-6 to embrace, understand, and support enterprise missions and programs. Therefore, we must collaboratively engage with our stakeholders to ensure that we meet requirements while following the disciplines established to govern C4&IT.

# CG-6 GOALS AND OBJECTIVES

## OVERVIEW

The following strategy consists of goals and objectives for CG-6 to accomplish over the next five years. Achievement of these goals and objectives will allow us to make substantive progress toward achieving the Commandant's strategic vision of the future. The goals are purposely broad with the objectives and initiatives focused primarily on a five-year timeframe. Building on the objectives, the CG-6 Performance Plan (Appendix A) identifies specific initiatives that will enable us to achieve the broader goals. Initiatives will be refined as we progress within objectives. As shown in Figure 2, the goals align to five central themes: technology, security, information, governance, and organizational excellence.

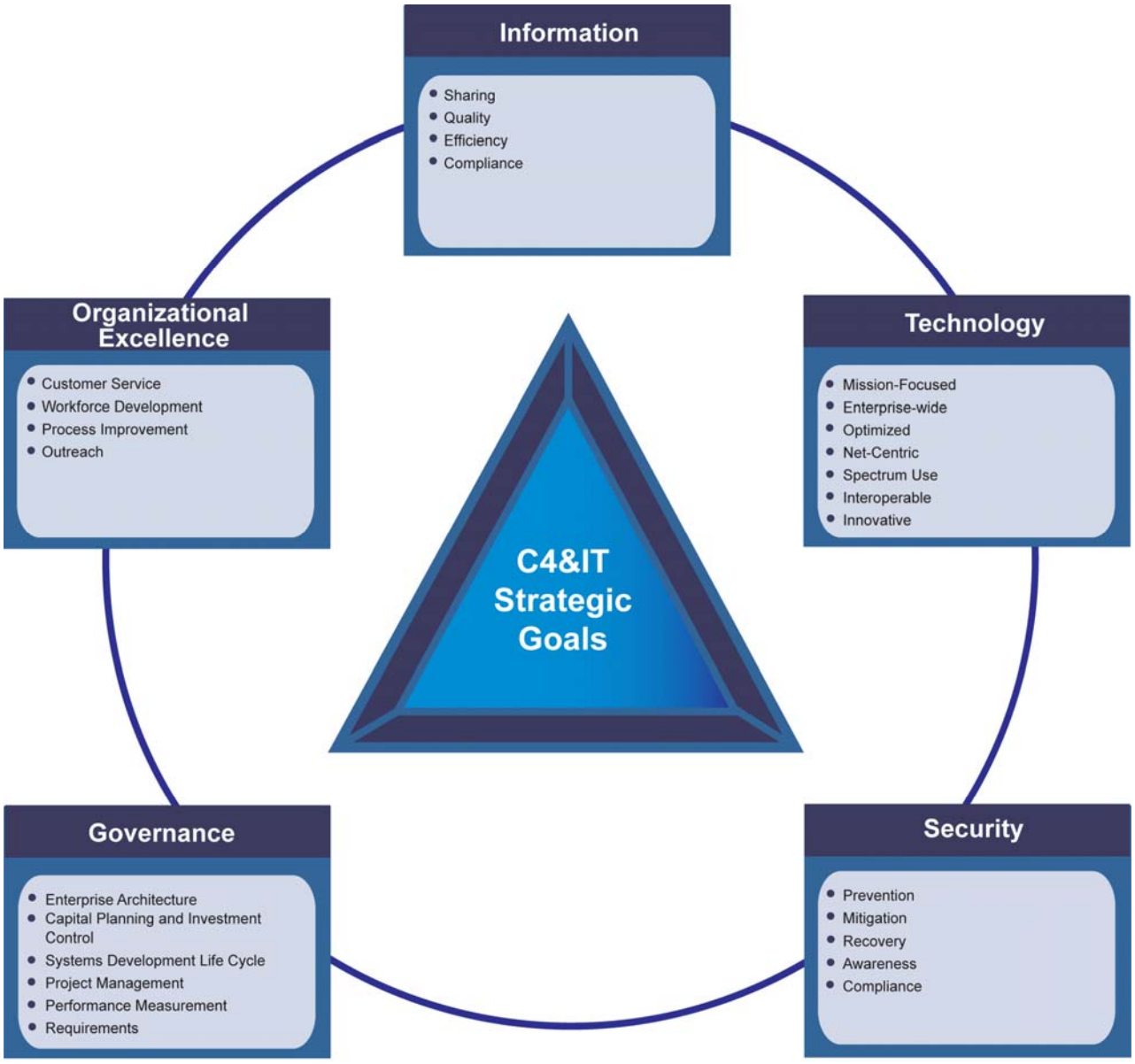


**Figure 2: CG-6 Goals Overview**

## GOAL 1: INFORMATION

Improve and encourage information sharing, quality, efficiency, and compliance throughout the Coast Guard.

### Intent

Coast Guard mission execution and tactical maneuvers rely on sharing current, valid, consistent, and comprehensive information. As such, our personnel must be able to manage the tactical, surveillance, and law enforcement information required to perform their duties. In addition, as the Coast Guard becomes more dependent on information sharing, it is increasingly important for us to be able protect information quality, enhance information efficiency, and ensure compliance with departmental guidance regarding the protection, transmission, and management of information. By doing so, we can help to improve mission execution and performance results.

### Objectives

1.1 Sharing: Enable information sharing by ensuring that information is visible, understandable, accessible, and interoperable throughout the Coast Guard and with external partners.

1.2 Quality: Promote information quality by establishing processes and procedures to make sure that the Coast Guard's information is valid, consistent, and comprehensive.

1.3 Efficiency: Provide improved support for the Coast Guard's business and mission by ensuring that Coast Guard information is requirements-based, non-duplicative, timely, and financially sound.

1.4 Compliance: Achieve the intent of Federal and departmental information management legislation and policies, including compliance with privacy, FOIA, and records management guidance.

## GOAL 2: TECHNOLOGY

Deliver mission-focused, interoperable, innovative, and net-centric C4&IT using enterprise-wide solutions, an optimized infrastructure, and electromagnetic spectrum efficiency.

### Intent

Coast Guard missions are increasingly dependent on the quality of our technology. Operators and support staff use C4&IT solutions throughout the Coast Guard to safeguard our oceans and waterways, enforce maritime laws, and serve our Nation. Interoperable, net-centric solutions provide our operators seamless communication with internal and external partners such as the DoD and its components; state, local, and tribal governments; and intelligence agencies. In addition, during times of war, our ability to transition from governmental responsibilities to defensive capabilities requires optimized and innovative C4&IT resources. To satisfy mission demands and operator needs, we must deliver mission-focused, interoperable, and net-centric C4&IT using enterprise-wide solutions, an optimized infrastructure, and electromagnetic spectrum efficiency.

### Objectives

2.1 Mission-Focused: Satisfy operator C4&IT requirements by delivering mission-focused solutions that improve mission execution and business processes, leverage enterprise solutions, and adhere to the CGEA.

2.2 Enterprise-wide: Define, implement, and enforce a standard set of enterprise-wide C4&IT systems, applications, products, and standards to enable interoperability, seamless communication, and consolidation.

2.3 Optimized: Optimize the Coast Guard C4&IT environment and reduce costs of operation by consolidating and integrating infrastructure in alignment with the Department's IT modernization and transition strategy.

2.4 Net-Centric: Leverage internet technologies to discover and exchange needed information in a timely manner.

2.5 Spectrum Use: Maximize the capabilities of Coast Guard operators through efficient and effective use of the electromagnetic spectrum.

2.6 Interoperable: Identify and replace stove-piped networks, systems, and applications with C4&IT solutions that are interoperable within the Coast Guard and with our partners, such as the DoD and its components; state, local, and tribal government; and intelligence agencies.

2.7 Innovative: Proactively apply innovative technologies and best practices to improve systems, close gaps, and set the pace for Government agencies and industry.

## GOAL 3: SECURITY

Prevent C4&IT security issues, such as cyber attacks and intrusions, and enhance C4&IT security mitigation, recovery, awareness, and compliance.

### Intent

As the Coast Guard becomes more dependent on networked communications to accomplish its mission, it is increasingly important to protect the integrity of the network and the information it stores and transmits. As such, any interruption, delay, or degradation in C4&IT capabilities can prevent access to critical information and processes. To protect our vital C4&IT resources, the Coast Guard must follow best practices, found within industry and Government, to create a layered defense for the systems that the Coast Guard relies on for mission execution. Additionally, we must develop the appropriate policies, acquire and field equipment, monitor our networks, train our workforce, and remain vigilant in our efforts to protect and maintain the integrity of the Coast Guard's computer and communications networks. By preventing C4&IT security issues and enhancing C4&IT security mitigation, recovery, awareness, and compliance, we can support international stability and national defense.

### Objectives

3.1 Prevention: Enhance C4&IT security by ensuring that proper safeguards and archiving processes are in place to ensure the confidentiality, integrity, availability, and privacy of information and compliance with legal requirements.

3.2 Mitigation: Improve the Coast Guard's ability to detect and respond to C4&IT security issues in a timely manner with minimal disruption to systems and the Coast Guard's ability to carry out its missions.

3.3 Recovery: Enhance Continuity of Operations Planning (COOP) and our ability to respond rapidly and effectively to security-related threats and natural disasters.

3.4 Awareness: Ensure security considerations are at the forefront of all C4&IT activities by developing acquisitions strategies and guidance to strengthen C4&IT security and build compliance.

3.5 Compliance: Increase Coast Guard compliance with the Federal Information Security Management Act (FISMA) to ensure that the technologies employed protect sensitive and confidential information, and sustain the privacy of Coast Guard personnel and American citizens.

## GOAL 4: GOVERNANCE

Enhance C4&IT governance to meet requirements and encourage effective enterprise architecture, capital planning and investment control, systems development life cycle, project management, and performance measurement processes.

### Intent

The fundamental purpose of enhancing C4&IT governance activities within the Coast Guard is to enable the strategic and tactical alignment of C4&IT investments, projects, and system development with the Coast Guard's priorities and goals. By doing so, we can maximize return on investment, mitigate risk, and ensure business and technical alignment to the Coast Guard Enterprise Architecture (CGEA). Additionally, sound C4&IT governance ensures that we effectively manage the cost, schedule, performance parameters, and configuration of Coast Guard investments and meet the requirements of the program sponsors.

### Objectives

4.1 Enterprise Architecture: Implement an accurate, current, and complete CGEA as the single source of C4&IT business and technology information throughout the Coast Guard to improve decision making.

4.2 Capital Planning and Investment Control: Establish effective policies and processes to govern the development and deployment of C4&IT throughout the Coast Guard and ensure effective oversight and financial management, and compliance with laws, policies, and directives.

4.3 Systems Development Life Cycle: Facilitate the use of the SDLC process to ensure collection and validation of requirements, adherence to the CGEA, and design and support of comprehensive solutions.

4.4 Performance Measurement: Establish and use relevant and meaningful C4&IT performance measures to ensure internal productivity and growth, and customer satisfaction.

4.5 Project Management: Enhance project management to ensure that we deliver C4&IT products and services to our customers on time and within budget using a common and repeatable process.

4.6 Requirements: Ensure that C4&IT solutions satisfy operator requirements by developing a disciplined requirements management strategy that establishes policies, practices, and procedures for capturing, storing, and managing requirements.

## GOAL 5: ORGANIZATIONAL EXCELLENCE

Achieve organizational excellence and provide superior customer service by continually developing our workforce, reaching out to internal and external stakeholders, and improving business processes.

### Intent

The Coast Guard depends on its people to perform its mission. Creating an environment that fosters organizational excellence begins with equipping, developing, and preparing our people for personal, professional, and organizational success. We can do this by providing them with the correct education, training, and professional experience needed to achieve C4&IT competencies. In addition, we must communicate the value of C4&IT and the CG-6 mission, vision, and strategy to enable our people to meet organizational goals. Organizational excellence also requires that processes are continually improved and streamlined to provide efficient and convenient access to C4&IT resources. The ultimate goal of organizational excellence is to deliver customer service that drives mission execution.

### Objectives

5.1 Customer Service: Ensure responsive and effective customer service by delivering comprehensive, accessible, reliable, and user-friendly solutions to meet or exceed C4&IT requirements.

5.2 Workforce Development: Equip our people for personal, professional, and organizational success and achieve our mission with a better trained, prepared, safe, and diverse workforce.

5.3 Process Improvement: Establish, institutionalize, and continually update processes to ensure streamlined, integrated, and optimized use of C4&IT resources.

5.4 Outreach: Communicate to the enterprise the value of C4&IT, and the CG-6 mission, vision, and strategy.

# THE WAY AHEAD

This Strategic Plan establishes the goals and objectives for CG-6, and demonstrates how they align with the overall Coast Guard and DHS strategic plans. Supporting this strategy, Appendix A: CG-6 Performance Plan, identifies specific initiatives, milestones, and key performance indicators to track our progress toward achieving these goals and objectives.

In essence, the CG-6 Performance Plan is the tactical plan for CG-6 that describes the initiatives that we are executing in support of CG-6 goals. All of the work we do as CG-6 should support one or more strategic goals and objectives. As such, all of our activities should fall within the scope of at least one of the initiatives described in the CG-6 Performance Plan. This alignment with the CG-6 strategic goals ensures that we are using our limited resources to satisfy the strategic goals of CG-6.

We will update both the C4&IT Strategic Plan and the CG-6 Performance Plan on a yearly basis. The Strategic Plan will cover a period of five years while the Performance Plan will contain initiatives that we can complete within a single year. In the Performance Plan, we will split multi-year initiatives into milestones to reflect a single year's effort. This will ensure that the plan contains items we can complete by the end of the year with sufficient detail to accurately track progress.

The Performance Plan also describes the key performance indicators that we will track to ensure that we are making progress toward achieving our goals. These measures will be included as part of an overall CG-6 "dashboard" that will be used to provide the status of all of our ongoing activities. We will describe the status of each of these measures as "red," "yellow," or "green," depending on the progress that we are making toward successfully completing the initiative. We will record incomplete items at the end of the year automatically as "red."

Together the C4&IT Strategic Plan and the CG-6 Performance Plan will provide our CG-6 community with clear direction on our goals and objectives, and a snapshot of our progress toward achieving these goals. Communicating this information to all of CG-6 will help us join together to provide the best possible service to our customers and better align our resources to support the Coast Guard's mission.


# CG-6 Performance Plan

FY08

# APPENDIX A: CG-6 PERFORMANCE PLAN

## GOAL 1: INFORMATION

### Initiatives

#### 1.1 Sharing

##### 1.1.1 Nationwide Automated Identification System (NAIS)

Exercise technical authority responsibilities in direct support of NAIS to enhance Maritime Domain Awareness (MDA). (Primary Point of Contact (POC): CG-64)

*Major Milestones*

FY08 Q3: Achieve full operating capability for Increment One

FY08 Q3: Complete request for proposal for Increment Two

FY08 Q4: Award Increment Two Contract

##### 1.1.2 Historical Archive Service (HAS) Prototype

Continue to support HAS, in partnership with the Research and Development (R&D) Center, for sharing of Automatic Identification System (AIS) data across multiple MDA partners within the Department of Homeland Security (DHS) and the Department of Defense (DoD). (Primary POC: CG-63/Operations Systems Center (OSC))

*Major Milestones*

FY08 Q3: Establish HAS at the OSC

*Key Performance Indicators*

- Database conversion of NAIS from SQLServer to SybaseIQ
- Significant reduction in required storage space (especially when backup and disaster recovery are factored in); at least one order of magnitude total reduction
- HAS able to produce six-month historical search in less than three seconds

##### 1.1.3 Defense Messaging System (DMS) Deployment

Deploy the DMS to all shoreside and shipboard military messaging users. (Primary POC: CG-62)

*Major Milestones*

FY08 Q3: Install and test DMS infrastructure using the Automated Message Handling System (AMHS) at Communications Area Master Station Atlantic (CAMSLANT) and Communications Area Master Station Pacific (CAMSPAC)

FY08 Q3: Test the DMS tactical solution (DMS Stand-Alone Proxy (SAP)) on CGC LEGARE (as a part of the Navy's overall testing)

FY08 Q4: Begin DMS field deployment to all shoreside users (will begin with District 9). Transition 30,000 Coast Guard messaging users to DMS by 10 January 2009.

*Key Performance Indicators*

- Maintain a green status on monthly DMS Report Card
- Less than two percent errors reported for Coast Guard DMS sites

1.1.4 Freedom of Information Act (FOIA) Compliance

Promulgate policy, educate staff, and monitor responses to ensure that the Coast Guard complies with FOIA legislation, regulations, legal precedents, and procedures. This includes processing appeals of adverse decisions to FOIA requests. (Primary POC: CG-61)

*Major Milestones*

FY08 Q4: Serve as POC for upcoming FOIA audit

Ongoing: Realize all aspects of the FOIA Improvement Plan

Ongoing: Complete requested personnel additions

*Key Performance Indicators*

- FOIA audit scorecard
- Reduction in backlog of FOIA appeals
- Requested additional personnel are onboard

1.1.5 Privacy Compliance

Continue to ensure Coast Guard systems are submitted for privacy review no later than at the 35 percent design phase and ensure any required privacy documents, specifically System of Records Notices (SORNs), are consolidated under existing Federal/DHS-wide SORNs and new DHS-wide SORNs, when appropriate, as to not duplicate processes. Ensure SORNs for systems significantly changed are updated, reissued, or retired on a case-by-case basis. (Primary POC: CG-61)

*Major Milestones*

Ongoing: Consolidate, update, reissue, or retire legacy SORNs

Ongoing: Continue review of systems to ensure that the collection, use, maintenance, and disclosure of Personally Identifiable Information (PII) is consistent with the applicable Privacy Threshold Analysis (PTA), Privacy Impact Assessment (PIA), SORN, and FISMA reporting requirements, and establish programmatic safeguards to protect PII

Ongoing: Continue to establish Coast Guard policy for myriad aspects of Privacy Compliance not yet published

Ongoing: Obtain billets and/or program augmentation to perform essential programmatic outreach activities

*Key Performance Indicators*

- Green score for legacy SORNs on DHS FISMA Report
- Decreased privacy incidents
- Increased training opportunities; delegation of authority to subordinate-level for processing of Privacy Act requests, complaints, redress, and Web site compliance issues
- Decreased PII holdings

## 1.2 Quality

### 1.2.1 Data Stewardship

Data Stewardship encompasses the overall management of information following Systems Development Life Cycle (SDLC) principles from creation through disposition. The Coast Guard requires policies and procedures to ensure that data is properly collected, used, maintained, archived, shared, and disclosed. This will help assure that civil liberties policies exist for the use of data mining. As such, key elements of this stewardship involve parameters of the Records Management and Privacy Programs. (Primary POC: CG-61)

*Major Milestones*

Ongoing: Schedule Coast Guard systems through the National Archives and Records Administration

Ongoing: Secure DHS Electronic Records Management System funding approval

*Key Performance Indicators*

- Ongoing initiative to appraise/schedule systems (ten projected per quarter)
- Quarterly measurement (via DHS Scorecard) identifying number of systems scheduled as well number of staff trained in Records Management

## 1.3 Efficiency

### 1.3.1 Enterprise Service Bus (ESB) Deployment

Continue our efforts to deploy an ESB for the Coast Guard. This includes the selection of a security eXtensible Markup Language (XML) gateway appliance for use within the CGDN+ and DMZ to protect the ESB as services are brought on board; and completion of the ESB's Certification and Accreditation (C&A). (Primary POC: CG-63/OSC)

*Major Milestones*

FY08 Q4: Purchase initial hardware and software infrastructure for the production ESB

*Key Performance Indicators*

- Security policies and authentication mechanisms deployed in production
- Ability to authenticate and authorize other non-Coast Guard/DHS users
- Production services used by multiple business processes

### 1.3.2 Metadata

Create and use a catalog of data characteristics to develop a lexicon or data dictionary and facilitate information sharing, use, and management. (Primary POC: CG-6B)

*Major Milestones*

FY08 Q4: Publish the Coast Guard Information Management Strategy

*Key Performance Indicators*

- On-time delivery of the Coast Guard Information Management Strategy

### 1.3.3 Data Registries

Use these automated resources to describe, document, protect, control, and access Coast Guard information. (Primary POC: CG-6B)

*Major Milestones*

FY08 Q4: Publish the Coast Guard Information Management Strategy

*Key Performance Indicators*

- On-time delivery of the Coast Guard Information Management Strategy

### 1.3.4 Segment Architecture

Support segments (program sponsors) with the development of business, data, and systems models; information exchange packages; and information requirements. (Primary POC: CG-6B)

*Major Milestones*

FY08 Q2: Complete SDLC for The Enterprise Architecture Management System (TEAMS)

FY08 Q3: Complete Certification and Accreditation (C&A) for TEAMS

*Key Performance Indicators*

- On-time delivery of TEAMS SDLC
- On-time delivery of TEAMS C&A

## 1.4 Compliance

### 1.4.1 Information Management Strategy

Institute a Coast Guard information management strategy to provide data standards and efficient processes for enterprise data collection, sharing, analysis, protection, and retention. (Primary POC: CG-6B)

*Major Milestones*

FY08 Q4: Publish the Coast Guard Information Management Strategy

*Key Performance Indicators*

- On-time delivery of the Coast Guard Information Management Strategy

### 1.4.2 Enterprise Data Management Office (EDMO)/Enterprise Geospatial Management Office (EGMO)

Continue to build the Coast Guard EDMO/EGMO, in alignment with the DHS EDMO/EGMO to establish the principles, policies, and practices for information sharing, quality, efficiency, and compliance. (Primary POC: CG-6B)

*Major Milestones*

FY08 Q1: Establish the EDMO and EGMO

FY08 Q4: Publish the Coast Guard Information Management Strategy

*Key Performance Indicators*

- On-time delivery of the Coast Guard Information Management Strategy

# GOAL 2: TECHNOLOGY

## Initiatives

### 2.1 Mission-Focused

**2.1.1** Requirements Validation Process

Leverage the Enterprise Architecture Board (EAB) process to validate customer requirements against the Coast Guard Enterprise Architecture (CGEA). (Primary POC: CG-6B)

*Major Milestones*

FY08 Q4: Finalize the EAB submission form

*Key Performance Indicators*

- Number of EAB reviews completed

2.1.2 Cutter Connectivity

Continue to deploy Command, Control, Communications, and Computer (C4) solutions to improve performance, increase bandwidth, and lower costs for underway cutters. (Primary POC: CG-65)

*Major Milestones*

FY08 Q3: Install Small Cutter Connectivity solution on all 110's (mixed cellular/satellite communications solution)

FY08 Q3 Develop cellular only solution for other small cutters

FY08 Q3: Develop cellular only installation plan for 87's

### 2.2 Enterprise-wide

2.2.1 Logistics Systems Modernization

Continue to develop the Coast Guard Logistics Information Management System (CG-LIMS) to transform the Coast Guard's logistics systems in support of a Coast Guard-wide common logistics business model. (Primary POC: CG-63)

*Major Milestones*

FY08 Q4: Complete all Logistics Information Management System (LIMS)/CG-LIMS transition activities

*Key Performance Indicators*

- Knowledge transfer from Integrated Coast Guard Systems (invaluable in assessing LIMS/eMESA future usability)
- Cost effective solution supporting all Preliminary Operational Requirements Document (PORD) requirements and common business model

- Successful achievement of exit criteria for next acquisition phase
- Proven, stable, and secure enterprise architecture design
- Achievement of project plan objectives
- Timely and effective roll out
- Delivery of increments on or ahead of schedule for logistics community

#### 2.2.2 Financial Systems Modernization

Continue to support the Coast Guard's financial systems modernization effort to ensure that the Coast Guard's financial systems comply with government accounting, auditing, and financial reporting regulations. (Primary POC: CG-63)

*Major Milestones*

FY08 Q4: Award and execute emergency Systems Development Agent (SDA) services contract

FY08 Q4 Complete final legal ruling on the financial support/development contract

*Key Performance Indicators*

- Budgeted Cost of Work Scheduled (BCWS)
- Budgeted Cost of Work Performed (BCWP)
- Difference between budgeted costs and actual or projected costs or difference between budgeted hours and actual or projected hours (variance)
- Acquisition strategy completed

#### 2.2.3 Military HR/Payroll Modernization

Continue to implement and upgrade Direct Access and PeopleSoft's Global Payroll Application to transform the Coast Guard's Military human resources and payroll systems in support of a Coast Guard-wide consolidated Human Resources Management System (HRMS). (Primary POC CG-63)

*Major Milestones*

FY08 Q4: Complete short term solutions for reconciliation of Global Pay and JUMPS

FY08 Q4: Complete acquisition plan for follow-on contract for development and maintenance services

*Key Performance Indicators*

- Short term solutions implemented
- Completion of acquisition plan
- Completion of SDLC required documents and testing
- Project work breakdown structure, earned value management, and reports from Contractor

## 2.3 Optimized

#### 2.3.1 Data Center Consolidation

Continue to support the DHS CIO's goal of Data Center consolidation. This includes

installation of Asset Discovery Tools at current Coast Guard Data Centers; migration of the Coast Guard's disaster recovery capabilities to the second DHS data center; procurement and installation of core Coast Guard infrastructure at Stennis (i.e. tape backup, storage, and monitoring); and completion of the prototype migration process. (Primary POC: CG-63/OSC)

*Major Milestones*

FY08 Q4: Deploy Coast Guard core infrastructure (tape backup, enterprise storage, and system monitoring) to Stennis

*Key Performance Indicators*

- Delivery of hardware to Stennis
- Set-up and testing of hardware at Stennis

### 2.3.2 Email/Active Directory Steward for DHS

Lead the development, deployment, and operation of a DHS-wide enterprise e-mail solution in support of the DHS CIO. (Primary POC: CG-6I)

*Major Milestones*

FY08 Q4: Complete Memorandum of Agreement between the Coast Guard and DHS for e-mail/Active Directory

FY08 Q4: Award and initiate EMRF contract

### 2.3.3 Email Server Consolidation

Consolidate 150 email servers deployed world-wide to 35 email servers in 7 locations. This effort will support the DHS requirement for consolidation, centralized management, and data-center-capable operations. (Primary POC: CG-63/TISCOM)

*Major Milestones*

No milestones scheduled for FY08.

### 2.3.4 Portal Consolidation

Deliver web-based data and applications via an enterprise Coast Guard Portal (CG Portal) that transcends any particular customer base. This organizational approach to consolidation of multiple portal platforms and disparate web-content delivery mechanisms will provide a single interface for information sharing with Active Duty and Reserve Personnel, Civilians, Auxiliarists, and the public. The CG Portal will serve as the single access point for enterprise content and Coast Guard applications, and a collaborative environment for information sharing between Coast Guard members and external industry partners. (Primary POC: CG-63/OSC)

*Major Milestones*

FY08 Q4: Deliver collaboration (Quickr and Sametime) functionality to all Active Directory users

FY08 Q4: Provide Quickr training and migration assistance to Microsite owners

*Key Performance Indicators*

- Replacement of Microsites with new collaboration environment that includes migration of Microsite participants and documents

- External Web site via FatWire Content Management System (CMS) to include all Directorate content and high level pages (December 2008)
- Migration of all CG Central Microsite content to Quickr
- Improved customer satisfaction rating for web services

### 2.3.5 Trusted Internet Connections (TIC) Consolidation

Reduce the number of TIC that Coast Guard personnel use to access the Internet by two.

*Major Milestones*

No milestones scheduled for FY08.

## 2.4 Net-Centric

### 2.4.1 Coast Guard Data Network (CGDN+) consolidation and integration with DHS OneNet

Consolidate and integrate the DHS OneNet computer network with CGDN+ while ensuring continued connectivity with the DoD's computer networks (NIPRNET and SIPRNET). This includes deployment of Multi Protocol Label Switching (MPLS) to meet the Secretary's goal on OneNet migration. (Primary POC: CG-62/TISCOM)

*Major Milestones*

FY08 Q4: Transition 60 percent of the Coast Guard to MPLS by 31 August 2008

FY08 Q4: Transition 75 percent of the Coast Guard to MPLS by 30 September 2008*

FY08 Q4: Install a VNE server, Tenable, and IP Sonar by 1 August 2008

FY08 Q4: Install two Security Operations Center (SOC) tools

*Key Performance Indicators*

- Units transitioned
- Network Operations Center (NOC)/SOC visibility established (VNE, Tenable, and IP Sonar installed)

*Constraints: Currently, the Coast Guard can not order MPLS circuits in Alaska, Guam, and several other isolated locations.

### 2.4.2 Classified Network Connectivity

Maintain and enhance connectivity with DoD and DHS classified networks. (Primary POC: CG-62/TISCOM)

*Major Milestones*

FY08 Q4: Upgrade connectivity from 256kbps to T1 speeds (a total of 71 upgrades are planned for project; 50 upgrades will be completed prior to 30 September 2008)

FY08 Q4: Upgrade connectivity from T1 to T3 (a total of 18 upgrades are planned)

FY08 Q4: Establish criteria for determining if upgrade is required and is funded by 30 September 2008*

*Key Performance Indicators*

- Increase in performance created by increasing bandwidth to sites

*Note: Fund for the actual circuit upgrade is only a part of the cost.

#### 2.4.3 Internet Protocol Version 6 (IpV6) Migration

Complete the Coast Guard's migration to IpV6 as mandated by the Office of Management and Budget (OMB) Memorandum 05-22, and in alignment with DoD and industry best practices. Migration to IpV6 will provide a network infrastructure that is more scaleable and secure, and enable advanced applications for communications and information sharing. (Primary POC: CG-62/TISCOM)

*Major Milestones*

See 2.4.1 "CGDN+ consolidation and integration with DHS OneNet"
(WAN upgrades are tied to OneNet transition)

*Key Performance Indicators*

- Wide Area Network (WAN) and Local Area Network (LAN) components that are IPv6 compatible

## 2.5 Spectrum Use

#### 2.5.1 Ku-Band Installation and Testing

Continue Ku-band installation and testing for Capital Cutters. (Primary POC: CG-62/TISCOM)

*Major Milestones*

FY08 Q3: Install prototype systems on Sherman and Forward

FY08 Q4: Complete prototype evaluation through September 2008

#### 2.5.2 Fleet Broadband Installation and Testing

Continue fleet broadband testing with INMARSAT. (Primary POC: CG-62/TISCOM)

*Major Milestones*

FY08 Q3: Install prototype on Dallas

FY08 Q4: Evaluate prototype through August 2008

#### 2.5.3 INMARSAT-B Global Beam Change

Transition the Coast Guard from large global beams to smaller regional beams. (Primary POC: CG-62/TISCOM)

#### 2.5.4 Telecommunications Manual (TCM) (Commandant Instruction Manual (CIM) 2000.3) Update

Rewrite the TCM to bring it up-to-date and better reflect current telecommunications practices and procedures. (Primary POC: CG-62/TISCOM)

*Major Milestones*

FY08 Q3: Distribute manual for concurrent clearance

FY08 Q3: Sign and promulgate CIM 2000.3 by the end of June 2008

### 2.5.5 Spectrum Frequency Advocacy

Support the development of policies and tools that use electromagnetic spectrum effectively in support of Coast Guard operations. Proactively engage international forums on the electromagnetic spectrum to advocate for global policies that benefit future Coast Guard capabilities. (Primary POC: CG-62/TISCOM)

*Major Milestones*

FY08 Q1: Attain International Telecommunications Union World Radio Conference (treaty conference) acceptance for AIS satellite detection allocation, and agree to establish port security competency at next conference

FY08 Q1: Implement DoD's radio interference reporting procedure Coast Guard-wide in an effective manner

FY08 Q2: Implement Coast Guard 800 MHz public safety interoperability policy

FY08 Q2: Publish Coast Guard VHF radio frequency handbook, implementing command and control, maritime safety, and public safety interoperability process Coast Guard-wide

FY08 Q2: Terminate autositor Automated Mutual-Assistance Vessel Rescue system (AMVER)/OBS services in LantArea and Kodiak without adverse reaction

FY08 Q2: Initiate and sponsor successful commelex conference to support Coast Guard Sector radio communication needs

FY08 Q3: Complete Stage 4 (Final) spectrum certification for C130 H and J radar

FY08 Q3: Obtain approval to negotiate an AIS coordination agreement with Mexico

FY08 Q4: Complete decision on exclusive allocation of remaining AIS frequency 161.975 MHz

## 2.6 Interoperable

### 2.6.1 Enterprise Architecture (EA) Products

Continue to develop, update, and maintain inventories of Coast Guard C4&IT products, standards, and systems to help define a common and interoperable set of C4&IT solutions and opportunities for consolidation and integration. (Primary POC: CG-6B)

*Major Milestones*

FY08 Q2: Publish CGEA Release 2

*Key Performance Indicators*

- Percentage increase in the number of EA products maintained
- Percentage increase in the number of systems documented since the last release

### 2.6.2 Maintain .mil/.gov Dual Presence

Continue to maintain the Coast Guard's dual .mil/.gov presence to ensure interoperability with our Federal government and DoD partners. (Primary POC: CG-62/TISCOM)

*Major Milestones*

FY08 Q4: Complete planning to reduce internet connections to two by 31 July 2008

*Key Performance Indicators*

- Coast Guard .mil presence maintained

### 2.6.3 Common Desktop/ Federal Desktop Core Configuration (FDCC)

Continue to migrate the Coast Guard's standard workstation to the more secure Vista operating system in support of FDCC baseline implementation and deployment as directed by OMB. (Primary POC: CG-63/TISCOM)

*Major Milestones*

FY08 Q4: Order hardware to support Coast Guard-wide Standard Image 6.0 with Vista migration

FY08 Q4: Develop draft plan for regional Image 6.0 deployment

FY08 Q4: Initiate Phase 1 of the Implementation Plan

*Key Performance Indicators*

- Increase in the number of deployed workstations that are Vista compliant

## 2.7 Innovative

### 2.7.1 Web 2.0 Strategy

Develop a strategy that defines how the Coast Guard can use Web 2.0 technologies (e.g. social-networking sites, wikis, blogs, and podcasts) to improve the Coast Guard's missions and operations; provide transparency to the public and interact with constituents; and enhance information sharing and collaboration within the Coast Guard and with partners, such as the Navy, Army, Air Force, and Border Patrol. (Primary POC: CG-63/OSC)

*Major Milestones*

FY08 Q4: Meet with CG-00 to capture the Commander's intent for Web 2.0

FY08 Q4: Develop plan to support the Commander's intent for Web 2.0

### 2.7.2 Technology Partnerships

Develop Memorandums of Understanding (MOUs), Memorandums of Agreement (MOAs), and other agreements with the Coast Guard R&D center and other inter- and intra-agency partners to transfer technologies, share costs, and develop streamlined and cutting edge C4&IT. (Primary POC: CG-6I)

*Major Milestones*

FY08 Q3: Initiate Coast Guard participation in the Navy's Systems Engineering Working Group

Ongoing: Continue to conduct interagency discussion on potential areas of collaboration

## GOAL 3 SECURITY

### Initiatives

## 3.1 Prevention

#### 3.1.1 Advanced Encryption Standard (AES) Migration Project

Move the Coast Guard from the current analog Data Encryption Standard (DES) to the new AES. This is a Federal mandate that must be accomplished by 31 December 2008. (Primary POC: CG-65/TISCOM)

*Major Milestones*

FY08 Q3: Complete full upgrade of District 17 units to AES capability

#### 3.1.2 Over-the-air-rekeying (OTAR) Implementation Project

Implement OTAR throughout the Coast Guard using a centralized key management facility (KMF) concept. (Primary POC: CG-62/TISCOM)

#### 3.1.3 PII Training

Ensure that all Coast Guard personnel are trained in safeguarding and handling PII, including reporting requirements for suspected or actual loss of PII. (Primary POC: CG-61)

*Major Milestones*

Ongoing: Continue to establish and publicize Coast Guard policy for myriad aspects of privacy compliance via mandatory tutorials (i.e. Generally Mandated Training) and other avenues

Ongoing: Obtain billets and/or program augmentation to perform essential outreach activities and policy development

*Key Performance Indicators*

- Reduced number of privacy incidents
- Increased training opportunities; delegation of authority to subordinate-level for processing of Privacy Act requests, complaints, redress, and Web site compliance issues
- Decreased PII holdings

#### 3.1.4 Privacy Compliance/Privacy Threshold Analyses (PTAs)

Continue to conduct PTAs for new or substantially updated systems to be reviewed and included in Trusted Agent FISMA. Accordingly, write Privacy Impact Assessments (PIAs) for submission to DHS (as required). (Primary POC: CG-61)

*Major Milestones*

Ongoing: Submit PTAs for inclusion in Trusted Agent FISMA, and PIAs as required

Ongoing: Continue review of systems to ensure collection, use, maintenance, and disclosure of PII is consistent with provisions of the Privacy Act and applicable PTAs, PIAs, SORN, and FISMA reporting requirements

Ongoing: Continue to establish Coast Guard policy for myriad aspects of privacy compliance as required

Ongoing: Obtain billets and/or program augmentation to perform essential functions and responsibilities

*Key Performance Indicators*

- Green score for DHS FISMA Report
- Decreased privacy incidents

#### 3.1.5 Common Access Card (CAC) and Single Sign-on

Leverage CAC authentication as part of the solution for Single Sign-on and to eliminate token use for the Coast Guard Remote Access Service (RAS). (Primary POC: CG-65/TISCOM)

*Major Milestones*

FY08 Q4: Complete design and testing; procure equipment for issue

## 3.2 Mitigation

#### 3.2.1 Computer Network Defense (CND) Capabilities

Establish CND capabilities that support protecting, monitoring, detecting, analyzing, and responding to unauthorized activity and unintentional user errors. Develop a professional CND workforce through improved training, doctrine, and exercises, and Tactics, Techniques, and Procedures (TTPs). (Primary POC: CG-62/TISCOM)

#### 3.2.2 Security Measures of Effectiveness (MOE)

Establish security MOE to identify and periodically assess the Coast Guard's ability to secure the network. (Primary POC: CG-62/TISCOM)

## 3.3 Recovery

#### 3.3.1 System Disaster Recovery Plans

Ensure that all C4&IT systems at OSC have a Disaster Recovery Plan. (Primary POC: CG-63/OSC)

*Major Milestones*

FY08 Q4: Initiate system disaster recovery plan discussions

## 3.4 Awareness

### 3.4.1 Security Guidance

Develop strategies and guidance to strengthen and synchronize Coast Guard and DHS efforts to secure C4&IT infrastructure, information, and systems. (Primary POC: CG-62)

*Major Milestones*

FY08 Q3: Create a draft Commandant Instruction (COMDTINST) to address NFR CG-IT-07-014 "Weaknesses in Requirements for Role-Based Training for IT Professionals"

### 3.4.2 Security Training

Ensure that all personnel complete the generally mandated security awareness training and develop automated end-user training. This includes greater information security training for our military and civilian IT specialists to ensure personnel are versed in information security practices and requirements. (Primary POC: CG-65)

*Key Performance Indicators*

- 100 percent complete for information systems security user awareness training for each FISMA year
- 100 percent complete for users with significant security responsibility training for each FISMA year
- 100 percent complete for contingency plan and incident response training for each FISMA year. This training correlates with National Institute of Standards and Technology (NIST) SP 800-53 CP-3 and IR-2 controls
- 96 percent overall FISMA training score (attains green for training)

## 3.5 Compliance

### 3.5.1 Certification & Accreditation Assessments (C&A)

Ensure timely and successful completion of C&A assessments in compliance with Title III of the E-Government Act (Public Law 107-347)/FISMA. (Primary POC: CG-65)

*Major Milestones*

FY08 Q3: Receive authority for point of presence connection to NIPRNET for Intercontinental United States (INCONUS) and Outside the Continental United States (OUTCONUS)

FY08 Q3: Convert from the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) to the Defense Information Assurance Certification and Accreditation Process (DIACAP)

Annual Q2: Complete annual renewal of NIPRNET point of presence approval

*Key Performance Indicators*

- Maintain C&A green status for FISMA reporting

### 3.5.2 Information Assurance (IA) Consolidation

Continue to consolidate IA activities under CG-62, to monitor the security of C4&IT infrastructure, information, and systems throughout the enterprise; support FISMA efforts; and improve the procedures, processes, and acquisition strategies required for IA. (Primary POC: CG-62)

*Major Milestones*

FY08 Q3: Begin NFR work transfer to CG-621 (monitor success, hire staff, and develop work plans)

### 3.5.3 Deepwater IA Oversight

Provide programmatic oversight as the technical authority and Designated Accreditation Authority (DAA) for Deepwater Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) systems and participate as a member of the Deepwater IA SGT. (Primary POC: CG-62)

## GOAL 4: GOVERNANCE

### Initiatives

### 4.1 Enterprise Architecture

#### 4.1.1 CGEA Development and Maintenance

Continue to develop, maintain, and release CGEA profiles, models, and inventories to enhance decision making through information transparency. (Primary POC: CG-6B)

*Major Milestones*

FY08 Q2: Publish CGEA Release 2

FY08 Q4: Support DHS Inspector General (IG) Audit of CGEA

*Key Performance Indicators*

- Percentage increase in the number of CGEA products maintained
- Percentage increase in the number of systems documented since the last release

#### 4.1.2 Enterprise Architecture Board (EAB)

Align C4&IT project investments to the CGEA through technical reviews. (Primary POC: CG-6B)

*Major Milestones*

Ongoing: Conduct EAB reviews

*Key Performance Indicators*

- Number of projects reviewed by the EAB

#### 4.1.3 Systems Engineering Technical Advisory Board (SETAB)

Establish the SETAB to facilitate the transfer of technical knowledge between the Coast Guard's three C4&IT Centers of Excellence. (Primary POC: TISCOM, OSC, and C2CEN)

*Major Milestones*

FY08 Q4: Draft charter to establish the SETAB

*Key Performance Indicators*

- On-time delivery of SETAB charter

#### 4.1.4 Information Governance Board

Establish an information governance board as the decision making authority for the creation and maintenance of information management principles, policies, and practices. (Primary POC: CG-6B)

*Major Milestones*
FY08 Q4: Publish the Coast Guard Information Management Strategy

*Key Performance Indicators*
- On-time delivery of the Coast Guard Information Management Strategy

## 4.2 Capital Planning and Investment Control

### 4.2.1 Governance Process Integration

Integrate multiple governance processes (i.e. Coast Guard acquisition processes, and DHS Enterprise Architecture Center of Excellence (DHS EACOE), EAB, IT Acquisition Review (ITAR), Major Systems Acquisition Manual (MSAM), and SDLC processes) into a singular streamlined governance process to select, acquire, use, maintain, and dispose of C4&IT investments. The process will use best practices for Capital Planning and Investment Control (CPIC) such as the Control Objectives for Information and related Technology (COBIT). (Primary POC: CG-6R)

*Major Milestones*
FY08 Q4: Identify all current governance processes and propose draft streamlined process for investment governance

*Key Performance Indicators*
- Total number of processes impacting C4&IT Investments
- Number of redundant data capture requirements
- Number of redundant data capture requirements eliminated

### 4.2.2 Portfolio Management Process

Initiate a portfolio management process and align ongoing projects and investments with the DHS IT Portfolio structure to ensure best strategic value to the Coast Guard. (Primary POC: CG-6R)

*Major Milestones*
FY08 Q3: Complete OMB 300 Submissions in accordance with DHS/OMB Guidance

FY08 Q4: Complete Exhibit 53 Submissions in accordance with DHS/OMB Guidance

*Key Performance Indicators*
- Portfolio numbers ($/%) (report to all Coast Guard stakeholders)
- Identification of Coast Guard POCs responsible for quarterly updates to the Coast Guard CIO regarding DHS Target Technologies

### 4.2.3 C4&IT Investment Review Board (IRB)

Deliver efficient and cost effective investment decisions that provide consistent enterprise-wide C4&IT resources. (Primary POC: CG-6R)

*Major Milestones*

FY08 Q4: Establish C4&IT Central Fund (AFC30)

FY08 Q4: Complete FY09 C4&IT enterprise-wide spend plan

FY08 Q4: Complete FY09 C4&IT Execution Stage (EXSTAGE) Request

FY08 Q4: Partner with all programs to build FY11 C4&IT Resource Proposals under IRB direction

FY08 Q4: Work with CG-69[1] and CG-9 to release the Chief of Contracting Office Alert regarding the execution of C4&IT contracts and need for CIO Approval

*Key Performance Indicators*

- Number of C4&IT investments included under Management of the CIO (report percent growth in numbers and funding)
- Number of C4&IT investments executed outside of IRB purview monthly (as identified by various sources, including DHS IT review and spend plan submissions)

#### 4.2.4 CG-9 Alignment

Work with CG-9 to define roles, responsibilities, policies, and practices for C4&IT acquisitions. (Primary POC: CG-6R/CG-69)

#### 4.2.5 IT Acquisition Reviews (ITAR)

Continue to leverage, institutionalize, and refine the ITAR Process.

*Major Milestones*

No Milestones scheduled for FY08.

## 4.3 Systems Development Life Cycle

#### 4.3.1 SDLC Development and Maintenance

Continue to leverage, institutionalize, and refine the SDLC Process. (Primary POC: CG-69)

*Major Milestones*

No Milestones scheduled for FY08.

## 4.4 Performance Measurement

#### 4.4.1 CIO Dashboard

Present C4&IT performance measures in an executive dashboard format for enhancing C4&IT awareness and management. (Primary POC: CG-6B)

[1] CG-69 is a proposed office under the new CG-6 Organization Structure.

*Major Milestones*
No milestones scheduled for FY08.

#### 4.4.2 Comprehensive set of C4&IT measures

Establish and institutionalize comprehensive, meaningful, and actionable performance measures to monitor C4&IT usage, requirements, and investment. (Primary POC: CG-6B)

*Major Milestones*
No milestones scheduled for FY08.

## 4.5 Project Management

#### 4.5.1 Coast Guard C4&IT Project Management Office Charter

Develop a charter to establish the PMO and utilize the Project Management Body of Knowledge (PMBoK) to develop principles, policies, and practices for project management and an Earned Value Management (EVM) methodology for the Coast Guard. (Primary POC: CG-69)

*Major Milestones*
No milestones scheduled for FY08.

## 4.6 Requirements

#### 4.6.1 Requirements Management

Ensure that C4&IT solutions satisfy customer requirements by developing a disciplined requirements management strategy that establishes policies, practices, and procedures for capturing, storing, and managing requirements. (Primary POC: CG-6B)

*Major Milestones*
FY08 Q2: Complete TEAMS SDLC

FY08 Q3: Complete C&A for TEAMS

*Key Performance Indicators*
- On-time delivery of TEAMS SDLC
- On-time delivery of TEAMS C&A

# GOAL 5: ORGANIZATIONAL EXCELLENCE

## Initiatives

### 5.1 Customer Service

#### 5.1.1 Center of Excellence (COE) Consolidation

Support the Coast Guard's transformation by consolidating the centers of excellence into an integrated C4&IT Service Center that will provide full life-cycle management and bi-level maintenance support for Coast Guard people, platforms, and systems. (Primary POC: CG-6I)

*Major Milestones*

FY08 Q4: Complete full stand-up of PreComDet for C4&IT Service Center

FY08 Q4: Initiate Transition Plan development

#### 5.1.2 Industry Best Practices Adoption and Execution

Continue to leverage best practices (i.e. Information Technology Infrastructure Library (ITIL), Capability Maturity Model Integration (CMMi), and Lean Six Sigma) to ensure the delivery of high-quality customer service. (Primary POC: CG-6I)

*Major Milestones*

FY08 Q3: Offer ITIL course to Coast Guard personnel

Ongoing: Distribute best practices to CG-6 personnel on a regular basis

### 5.2 Workforce Development

#### 5.2.1 C4&IT Professional Development

Provide guidance to help develop our personnel and allow for success as both a Coast Guard Officer and an IT Specialist/Engineer. This includes identifying top reasons for C4&IT Workforce loss (i.e. retirement, other specialties, and private sector) and factors that comprise an officer's career, and analyzing what factors may have more impact on promotion (i.e. whether an officer had post-graduate school, whether they had homesteaded). (Primary POC: CG-6R)

*Major Milestones*

Ongoing: Promulgate C4&IT Officer's Handbook

Ongoing: Promulgate Force notes (minimum quarterly)

*Key Performance Indicators*

- Promotion board results for C4&IT Officers

### 5.2.2 Individual Development Plans (IDPs)

Create and update IDPs to help employees develop their skills, achieve their career goals, and further the CG-6 mission. (Primary POC: CG-6R)

*Major Milestones*

FY08 Q3: Develop a list of C4&IT personnel requiring IDPs

FY08 Q4: Confirm completion of IDPs for identified personnel

*Key Performance Indicators*

- Percentage of members that have IDPs complete within four years of services

### 5.2.3 Organization Assessment Surveys (OAS)

Regularly conduct surveys to review the workforce climate for the C4&IT specialty against all Coast Guard offices to highlight areas that CG-6, individual programs, and workforce managers might be able to address and improve. (Primary POC: CG-6R)

*Major Milestones*

FY08 Q3: Implement departure interview process

FY08 Q3: Review most recent survey and develop draft survey with updates as needed

FY08 Q4: Deploy survey (liaison with CG-1/481)

*Key Performance Indicators*

- Benchmark comparison of OAS results (use first survey as benchmark and compare to most recent results)
- CG-6 results from most recent Coast Guard OAS

## 5.3 Process Improvement

### 5.3.1 Facility and Workspace Improvement

Create an optimized work environment and increase personnel performance by improving individual workspaces, work stations, and Coast Guard facilities to promote the safety and technical needs of personnel. (Primary POC: CG-6)

### 5.3.2 Policy and Doctrine Development

Build and update C4&IT policies and doctrines that reflect streamlined and comprehensive C4&IT requirements and security concerns; and align with DHS, DoD, and Other Government Agencies (OGAs). (Primary POC: CG-6B)

*Major Milestones*

FY08 Q4: Kick-off IT Integration Mission Action Plan (MAP) project for Milestone 3.1: IT Governance

FY08 Q4: Participate in the Coast Guard Doctrine Study Group (DSG)

*Key Performance Indicators*

- On-time delivery of IT Integration MAP project kick-off

## 5.4 Outreach

### 5.4.1 CG-6 Strategic Communications Plan

Develop and implement a strategic communications plan to ensure that we communicate regularly about C4&IT initiatives, value, mission, and strategy. (Primary POC: CG-6D)

### 5.4.2 C4&IT and Engineering Outreach Events

Conduct outreach events to provide open opportunities for members of our specialties and ratings to ask career questions, identify deficiencies in organizational performance, and provide information on new initiatives, training, and education opportunities. (Primary POC: All)

# APPENDIX B: STRATEGIC ALIGNMENT MATRICES

## ALIGNMENT OF DHS CIO GOALS AND USCG C4&IT GOALS

| DHS CIO GOALS \ USCG C4&IT GOALS | Information | Technology | Security | Governance | Organizational Excellence |
|---|---|---|---|---|---|
| Goal 1<br>Continue cyber security improvements | ✓ | ✓ | ✓ | | |
| Goal 2<br>Drive IT operational efficiencies, improvements, and resiliency | | ✓ | | ✓ | ✓ |
| Goal 3<br>Align IT planning and budgeting with procurement activities and the enterprise architecture | ✓ | ✓ | ✓ | ✓ | ✓ |
| Goal 4<br>Establish a foundation for information sharing, data collection, and integration | ✓ | ✓ | | ✓ | ✓ |
| Goal 5<br>Establish and govern a portfolio of cross-departmental IT capabilities to support the DHS mission and management objectives | ✓ | ✓ | | ✓ | ✓ |

Source: DHS OCIO Strategic Plan FY 2007-2011

## ALIGNMENT OF USCG STRATEGIC PRIORITIES FOR FY09 AND USCG C4&IT GOALS

| USCG C4&IT GOALS / USCG STRATEGIC PRIORITIES FOR FY09 | Information | Technology | Security | Governance | Organizational Excellence |
|---|---|---|---|---|---|
| Recapitalizing Operating Assets and Sustaining Aging Infrastructure | | ✓ | | ✓ | |
| Enhancing Marine Safety | ✓ | ✓ | ✓ | ✓ | ✓ |
| Improving Command and Control Capabilities | ✓ | ✓ | ✓ | | ✓ |
| Polar Presence and Capabilities | ✓ | ✓ | ✓ | | ✓ |
| Establishing Comprehensive Intelligence and Awareness Regimes | ✓ | ✓ | ✓ | ✓ | |

Source: USCG Posture Statement (2008)

## ALIGNMENT OF THE USCG STRATEGY FOR SAFETY, SECURITY AND STEWARDSHIP AND USCG C4&IT GOALS

| USCG C4&IT GOALS / USCG STRATEGY FOR SAFETY, SECURITY & STEWARDSHIP | Information | Technology | Security | Governance | Organizational Excellence |
|---|---|---|---|---|---|
| Strengthen regimes for the U.S. maritime domain | | | ✓ | ✓ | |
| Achieve awareness in the Maritime Domain | ✓ | ✓ | ✓ | ✓ | |
| Enhance unity of effort in maritime planning and operations | ✓ | ✓ | ✓ | ✓ | ✓ |
| Integrate Coast Guard capabilities for national defense | ✓ | ✓ | ✓ | ✓ | |
| Develop a national capacity for Marine Transportation System recovery | ✓ | ✓ | ✓ | ✓ | |
| Focus international engagement on improving maritime governance | ✓ | ✓ | ✓ | ✓ | |

Source: USCG Strategy for Maritime Safety, Security, and Stewardship (2007)

## ALIGNMENT OF THE DOD INFORMATION SHARING STRATEGY AND USCG C4&IT GOALS

| USCG C4&IT GOALS / DoD INFORMATION SHARING STRATEGY | Information | Technology | Security | Governance | Organizational Excellence |
|---|---|---|---|---|---|
| Promote, encourage, and incentivize sharing | ✓ | ✓ | ✓ | ✓ | ✓ |
| Achieve an extended enterprise | ✓ | ✓ | ✓ | ✓ | |
| Strengthen agility, in order to accommodate unanticipated partners and events | ✓ | ✓ | ✓ | ✓ | ✓ |
| Ensure trust across organizations | ✓ | ✓ | ✓ | ✓ | |

Source: DoD Information Sharing Strategy (2007)

# APPENDIX C: ACRONYMS

| | |
|---|---|
| AES | Advanced Encryption Standard |
| AIS | Automatic Identification System |
| AMHS | Automated Message Handling System |
| AMVER | Automated Mutual-assistance Vessel Rescue system |
| BCWP | Budgeted Cost of Work Performed |
| BCWS | Budgeted Cost of Work Scheduled |
| C&A | Certification and Accreditation |
| C4 | Command, Control, Communications, and Computers |
| C4ISR | Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance |
| C4&IT | Command, Control, Communications, Computers, and Information Technology |
| CAC | Common Access Card |
| CAMSLANT | Communications Area Master Station Atlantic |
| CAMSPAC | Communications Area Master Station Pacific |
| CAO | Chief Acquisition Officer |
| CG | Coast Guard |
| CG Portal | Coast Guard Portal |
| CG-LIMS | Coast Guard Logistics Information Management System |
| CGC | Coast Guard Cutter |
| CGDN+ | Coast Guard Data Network |
| CGEA | Coast Guard Enterprise Architecture |
| CIAO | Commandant's Intent Action Order |
| CIM | Commandant Instruction Manual |
| CIO | Chief Information Officer |
| CIRC | Computer Incident Response Center |
| CMMi | Capability Maturity Model Integration |
| CMS | Content Management System |
| CND | Computer Network Defense |
| COBIT | Control Objectives for Information and related Technology |
| COE | Center of Excellence |
| COMDINST | Commandant Instruction |
| COOP | Continuity of Operations Planning |
| CPIC | Capital Planning and Investment Control |
| CUI | Controlled Unclassified Information |
| DAA | Designated Accreditation Authority |
| DES | Data Encryption Standard |
| DHS | Department of Homeland Security |
| DIACAP | Defense Information Assurance Certification and Accreditation Process |
| DITSCAP | DoD Information Technology Security Certification and Accreditation Process |
| DMS | Defense Messaging System |
| DoD | Department of Defense |
| DOG | Deployable Operations Group |
| DOJ | Department of Justice |
| EA | Enterprise Architecture |
| EAB | Enterprise Architecture Board |
| EACOE | Enterprise Architecture Center of Excellence |
| eCG | Electronic Coast Guard |
| EDMO | Enterprise Data Management Office |
| EGMO | Enterprise Geospatial Management Office |
| ESB | Enterprise Service Bus |

| | |
|---|---|
| EVM | Earned Value Management |
| EXSTAGE | Execution Stage |
| FDCC | Federal Desktop Core Configuration |
| FEMA | Federal Emergency Management Agency |
| FISMA | Federal Information Security Management Act |
| FOIA | Freedom of Information Act |
| FY | Fiscal Year |
| HAS | Historical Archive System |
| HRMS | Human Resources Management System |
| HSPD | Homeland Security Presidential Directive |
| IDPs | Individual Development Plans |
| IA | Information Assurance |
| ICGS | Integrated Coast Guard Systems |
| IG | Inspector General |
| INCONUS | Intercontinental United States |
| IP | Internet Protocol |
| IPv6 | Internet Protocol Version 6 |
| IT | Information Technology |
| ITAR | Information Technology Acquisition Review |
| ITIL | Information Technology Infrastructure Library |
| KMF | Key Management Facility |
| LAN | Local Area Network |
| LIMS | Logistics Information Management System |
| MAP | Mission Action Plan |
| MD | Management Directive |
| MDA | Maritime Domain Awareness |
| MIRP | Maritime Infrastructure Recovery Plan |
| MPLS | Multi-protocol Label Switching |
| MOE | Measures of Effectiveness |
| MOTR | Maritime Operational Threat Response Plan |
| MOA | Memorandum of Agreement |
| MOU | Memorandum of Understanding |
| MSAM | Major Systems Acquisition Manual |
| NAIS | Nationwide Automated Identification System |
| NARA | National Archives and Records Administration |
| NIPRNET | Unclassified but Sensitive Internet Protocol Router Network (formerly called the Non-Classified Internet Protocol Router Network) |
| NIST | National Institute of Standards and Technology |
| NMS | National Maritime Strategy |
| NOC | Network Operations Center |
| NSPD | National Security Presidential Directive |
| NSMS | National Strategy on for Maritime Security |
| OAP | Ocean Action Plan |
| OAS | Organizational Assessment Survey |
| OCIO | Office of the Chief Information Officer |
| OGAs | Other Government Agencies |
| OMB | Office of Management and Budget |
| ORD | Operational Requirements Document |
| OSC | Operations Systems Center |
| OTAR | Over-the-air-rekeying |
| OUTCONUS | Outside the Continental United States |
| PIA | Privacy Impact Assessment |
| PII | Personally Identifiable Information |
| PMBoK | Project Management Book of Knowledge |

| | |
|---|---|
| PMO | Project Management Office |
| PNT | Position Navigation and Timing |
| POC | Point of Contact |
| PORD | Preliminary Operational Requirements Document |
| PSB | Products and Standards Board |
| PTA | Privacy Threshold Analysis |
| PTAs | Privacy Threshold Analyses |
| Q1,2,3,4 | Quarter one, two, three, four |
| R&D | Research and Development |
| RAP | Remedial Action Program |
| RAS | Remote Access Service |
| RF | Radio Frequency |
| RSS | Real Simple Syndication |
| SAP | Stand-Alone Proxy |
| SDA | Systems Development Agent |
| SDLC | Systems Development Life Cycle |
| SETAB | Systems Engineering Technical Advisory Board |
| SIPRNET | Secure Internet protocol Router Network |
| SOA | Service Oriented Architecture |
| SOC | Security Operations Center |
| SOR | System of Record |
| SORN | System of Record Notice |
| SPAWAR | Space & Naval Warfare Systems Command |
| TCM | Telecommunications Manual |
| TEAMS | The Enterprise Architecture Management System |
| TIC | Trusted Internet Connections |
| TISCOM | Telecommunications & Information Systems Command |
| TTP | Tactics, Techniques, and Procedures |
| USCG | U.S. Coast Guard |
| WAN | Wide Area Network |
| WBS | Work Breakdown Structure |
| XML | eXtensible Markup Language |

# APPENDIX D: DEFINITIONS

| | |
|---|---|
| **Command, Control, Communications Computers, and Information Technology** | Command, Control, Communications, Computers, and Information Technology (C4&IT) consists of any equipment or interconnected system or subsystem of equipment, or technique used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of digital, voice, or video data or information to the appropriate levels of command. This includes command and control networks, common operational picture systems, information assurance services, communication products and standards, computers, ancillary equipment, software, firmware, procedures, services (including support services), and related resources. |
| **Enterprise Architecture** | Enterprise Architecture (EA) is the discipline that synthesizes key business and technology information across the organization to support better decision making. EA provides useful and usable information products and governance services to the end-user while developing and maintaining the current and target (to-be) architectures and transition plan for the organization. The information in the EA, includes: results of operations, business functions and activities, information requirements, supporting applications and technologies, and security. |
| **Measure of Effectiveness** | A measure of effectiveness (MOE) is a criterion used to assess changes in system behavior, capability, or operational environment that is tied to measuring the attainment of an end state, achievement of an objective, or creation of an effect. |
| **Service Oriented Architecture** | Service Oriented Architecture (SOA) is a computer systems architectural style for creating and using business processes, packaged as services, throughout their lifecycle. SOA also defines and provisions the IT infrastructure to allow different applications to exchange data and participate in business processes. These functions are loosely coupled with the operating systems and programming languages underlying the applications. SOA separates functions into distinct units (services), |

which can be distributed over a network and can be combined and reused to create business applications. These services communicate with each other by passing data from one service to another, or by coordinating an activity between two or more services. SOA concepts are often seen as built upon and evolving from older concepts of distributed computing and modular programming.

**Systems Development Life Cycle**

Systems Development Life Cycle (SDLC) is defined by the U.S. Department of Justice (DOJ) as a software development process, although it is also a distinct process independent of software or other information technology considerations. It is used by a systems analyst to develop an information system, including requirements, validation, training, and user ownership through investigation, analysis, design, implementation, and maintenance. SDLC is also known as information systems development or application development. An SDLC should result in a high quality system that meets or exceeds customer expectations, within time and cost estimates, works effectively and efficiently in the current and planned information technology infrastructure, and is cheap to maintain and cost-effective to enhance.

# APPENDIX E: REFERENCES


Department of Defense (2007). *Joint Publication 1-02, "DoD Dictionary of Military and Associated Terms"*. As amended through 17 October 2007. Retrieved 20 March 2008, from http://www.dtic.mil/doctrine/jel/doddict/

Department of Homeland Security (2004). *Securing Our Homeland, U.S. Department of Homeland Security Strategic Plan.*

Department of Homeland Security (2007). *Office of the Chief Information Officer Strategic Plan: Fiscal Years 2007-2011.*

Executive Office of the President (2005). *The National Strategy for Maritime Security*. Retrieved 21 May 2008, from http://www.whitehouse.gov/homeland/maritime-security.html#intro.

Executive Office of the President (2007). *The National Strategy for Homeland Security*. Retrieved 21 May 2008, from http://www.whitehouse.gov/homeland/maritime-security.html#intro.

Kurzweil, Ray (2001). *Essay: The Law of Accelerating Returns.* Retrieved 30 March 2008, from http://www.kurzweilai.net/meme/frame.html?main=/articles/art0134.html.

U.S. Coast Guard. *Commandant's Intent Action Orders*.

U.S. Coast Guard (2007). *The U.S. Coast Guard Strategy for Maritime Safety, Security, and Stewardship*.

U.S. Coast Guard (2008). *The U.S. Coast Guard Enterprise Architecture Executive Handbook*. Retrieved 15 May 2008, from http://cgea.uscg.mil/

NOTES


ASSISTANT COMMANDANT FOR C4&IT
N
W
E
S
CG-6


TELECOMMUNICATION & INFORMATION SYSTEMS COMMAND
U.S. COAST GUARD
ALEXANDRIA, VIRGINIA


OPERATIONS SYSTEMS CENTER
TEAMWORK
INITIATIVE
INNOVATION
USCG


U.S. COAST GUARD COMMAND AND CONTROL
ENGINEERING CENTER


UNITED STATES COAST GUARD
HOME OF THE LORANIMALS
LORAN SUPPORT UNIT